ISSN 2500-4255

УДК 343.98
DOI 10.17150/2500-4255.2020.14(3).471-480

О ВОЗМОЖНОСТЯХ КРИМИНАЛИСТИЧЕСКОЙ ГАБИТОСКОПИИ ПРИ РЕАЛИЗАЦИИ МЕР ПРОТИВОДЕЙСТВИЯ СОВРЕМЕННОЙ КИБЕРПРЕСТУПНОСТИ

А.А. Протасевич, Е.И. Фойгель
Байкальский государственный университет, г. Иркутск, Российская Федерация

Информация о статье

Дата поступления
15 апреля 2020 г.

Дата принятия в печать
25 июня 2020 г.

Дата онлайн-размещения
30 июня 2020 г.

Ключевые слова
Габитоскопия; внешний облик; цифровой образ; поведенческая биометрия; биометрия поведения; стилометрия; клавиатурный почерк; цифровой почерк; цифровые следы; расследование киберпреступлений; криминалистическая техника

Аннотация. Статья посвящена обзору современных возможностей криминалистической габитоскопии в условиях глобальной цифровизации. Методические рекомендации по расследованию и раскрытию киберпреступлений должны основываться на серьезной научно-методологической основе, в качестве которой может выступить криминалистическая габитоскопия. К числу свойств внешнего облика человека в условиях глобальной цифровизации и необходимости использовать виртуальные каналы общения (программы видео-конференц-связи) целесообразно добавить воспринимаемость как способность отдельных характеристик внешнего облика быть распознанными субъектом восприятия (с помощью органов чувств человека или технических устройств). В этой связи представляется, что внешний облик человека — это сложная система элементов, в совокупности складывающихся во внешность человека — образ, который зрительно воспринимается другими людьми и техническими устройствами. С учетом воспринимаемости внешнего облика человека его общефизические признаки, помимо традиционных, будут включать геометрию рук, рисунок вен на ладонных поверхностях, пальцевую термограмму, геометрию лица и черепа и др., имеющие высокое криминалистическое значение. Однако в связи с современными российскими условиями санитарно-эпидемиологического (ношение медицинских масок, перчаток), климатического (укутывание лиц шарфами, повязками), культурного (ношение женщинами национальных костюмов, скрывающих лицо, следование мужчин моде на щетину или бороду) характера, а также уже разработанными преступниками методами фальсификации анатомических признаков и противодействия криминалистическим технологиям наиболее перспективным представляется исследование динамических признаков внешнего облика в виде цифрового поведения. К числу таких признаков в первую очередь необходимо отнести стилометрию (клавиатурный почерк) — набор динамических характеристик при нажатии на клавиши клавиатуры компьютера, включающий в себя систему подсознательных автоматических действий, привычных пользователю. Кроме этого, в число наиболее значимых признаков цифрового поведения необходимо включить цифровой почерк, жестикуляцию, мимику и движение губ.

ON THE SCOPE OF CRIMINALISTIC HABITOSCOPY IN THE IMPLEMENTATION OF MEASURES AGAINST MODERN CYBER CRIME

Alexander A. Protasevich, Elena I. Foygel
Baikal State University, Irkutsk, the Russian Federation

Article info

Received
2020 April 15

Accepted
2020 June 25

Available online
2020 June 30

Abstract. The article presents an overview of modern possibilities of criminalistic habitoscopy in the conditions of global digitization. Methodological recommendations on the investigation and solution of cybercrimes should have a serious research and methodological basis, and criminalistic habitoscopy could provide such a basis. In the situation of global digitization and the use of virtual channels of communication (video conference calls), the characteristics of a person's outward features should include perceptibility, or the ability of the subject of perception (human sense organs or technical devices) to identity specific features of that person's look. In connection with this, the authors claim that a person's outward features are a complex system of elements that together form his or her appearance — an image that is visually perceived by other people or by devices. Taking into account the perceptibility of a person's outward look, his or her general physical features, besides the traditional ones, will include the geometry of hands, the vein structure on palm surfaces, finger

ISSN 2500-4255

Keywords
Habitoscopy; appearance; digital image; behavioral biometrics; biometrics of behavior; stylometry; keyboard handwriting; digital handwriting; digital traces; cybercrime investigation; forensic technology

thermogram, face and skull geometry, etc., all of which have a high criminalistic value. However, considering the current sanitary and epidemiology measures undertaken in Russia (wearing medical masks and gloves), climate (covering faces with scarves and kerchiefs) and cultural (women wearing national clothes that cover their faces, men with stubble or a beard) specifics, as well as the methods of falsifying anatomical features and counteracting criminalistic technologies already developed by the criminals, the authors view the research of the dynamic characteristics of a person's outward appearance in the form of digital behavior as the most perspective area. These characteristics primarily concern stylometry (keyboard handwriting) — a set of dynamic characteristics of pressing keys on a computer keyboard, which includes a system of subconscious automatic actions habitual to the user. Besides, the most relevant features of digital behavior should include digital handwriting, gestures, facial expression and lip movement.

Глобальная цифровизация, проникающая во все сферы общественной жизни, неожиданно стала основным средством решения серьезных проблем, с которыми столкнулось человеческое общество в реалиях пандемии новой коронавирусной инфекции COVID-19. Своевременно принятая Стратегия развития информационного общества в Российской Федерации на 2017–2023 годы, утвержденная указом Президента Российской Федерации от 9 мая 2017 г. № 203, закрепила необходимость обеспечения всеобщего доступа к информационным и коммуникационным технологиям и интенсификации использования самих технологий, обусловив их широкое внедрение в большинство сфер общественной жизни. Применение активно появляющихся в последнее время научных разработок требует соответствующего научного обоснования. Не стала исключением и криминалистическая наука. Научные исследования в области криминалистической методики, в частности в сфере создания и совершенствования методики расследования киберпреступлений [1], тактики производства следственных действий в процессе расследования [2], находятся на самом высоком уровне развития, обеспечивая правоохранительную практику новыми способами и методами собирания, исследования и использования цифровых следов.

Однако представляется, что научно-методологические основы фундаментальных знаний предъявляют свои требования к систематизации создаваемого научного продукта. Криминалистическая методика, являясь четвертым, заключительным разделом криминалистики, обобщает криминальный опыт совершения отдельных видов преступления и практику их расследования [3, с. 9], аккумулирует достижения предыдущих трех разделов, адаптированных для расследования и раскрытия отдельных видов и групп преступлений. Ученые, называя криминалистическую методику конечным продуктом криминалистики, особенной частью криминалистики, подчеркивают частный характер создаваемых научных положений и разрабатываемых на их основе рекомендаций по отношению к общим положениям теории и методологии криминалистики, криминалистической техники и криминалистической методики. Таким образом, структура криминалистической науки закономерно обосновывает появление частных криминалистических рекомендаций на основе общих положений, являющихся научным базисом для дальнейшей конкретизации и развития. В этой связи вполне убедительными представляются предложения профессора Е.Р. Россинской о формировании новой частной криминалистической теории — теории компьютерно-информационного обеспечения криминалистической деятельности, объектом которой являются, с одной стороны, сами компьютерные средства и системы как носители разыскной и доказательственной криминалистически значимой информации, а с другой — система действий и отношений в механизмах преступлений с использованием компьютерных средств и систем, а также криминалистических компьютерных технологий выявления, фиксации, изъятия, сохранения, исследования и использования криминалистически значимой доказательственной и ориентирующей информации [4, с. 195]. Необходимость в создании научно-методологического базиса ведения собственно криминалистических разработок либо использования в криминалистике достижений точных наук продиктована логикой научного знания, а также требованиями научной обоснованности к практическим рекомендациям, применяемым в процессе выявления, расследования, раскрытия и предотвращения преступлений. Таким образом, теория компью-

терно-информационного обеспечения криминалистической деятельности имеет фундаментальный характер и создает предпосылки для совершенствования основных разделов криминалистики — техники, тактики и методики.

Однако практические рекомендации по производству отдельных следственных действий, направленных на собирание, исследование, оценку и использование цифровых следов, в расследовании преступлений в сфере информационных технологий до сих пор не получили четко обозначенной позиции в структуре криминалистической техники, а ограничены лишь трасологией: многие авторы предлагают наряду с общепринятыми в трасологии следами-отображениями, следами-предметами и следами-веществами выделять цифровые следы [5], виртуальные следы, информационные следы, и, как следствие, даже выделять такой подраздел, как кибертрасология [6, с. 43].

Вполне разделяя необходимость выделения категории цифровых следов, позволим себе все же обратить внимание на раздел криминалистической техники, который незаслуженно считается наименее подверженным глобальной цифровизации. Речь идет о криминалистической габитоскопии, традиционное восприятие которой заключается в возможностях криминалистического исследования внешнего облика. Это вполне закономерно, поскольку теоретические основы криминалистической габитоскопии были заложены французским криминалистом Альфонсом Бертильоном еще в конце XIX столетия, когда им был разработан и предложен метод составления словесного портрета. Несмотря на то что основы данной методики, унифицированные и уточненные в 1902 г. Рудольфом Арчибальдом Рейссом, востребованы и в настоящие дни, традиционное понимание криминалистической габитоскопии с учетом современных реалий нуждается в некотором пересмотре.

Предмет криминалистической габитоскопии был сформирован профессором А.М. Зининым и заключается в установлении закономерностей, обусловливающих природу внешнего облика человека, проявляющихся в его свойствах, а также в определении закономерностей собирания, исследования и использования данных о внешнем облике человека с помощью разработанных для этих целей методов и средств [7, с. 15].

Внешний облик — это совокупность зрительно воспринимаемых признаков, характеризующих внешность человека [8, с. 24]. Среди основных свойств внешнего облика человека выделяют индивидуальность, относительную устойчивость и рефлекторность.

Индивидуальность внешнего облика представляет собой отличие основных элементов внешности человека от иных людей. Несмотря на то что в мире зачастую встречаются внешне очень похожие люди (близнецы, так называемые двойники), говорить о тождественности внешнего облика таких людей нельзя. Совпадение части признаков не означает равности, тем более что совпадают, как правило, наиболее общие зрительно воспринимаемые элементы. Выраженность отдельно взятых признаков у таких лиц разная, что исключает полную тождественность восприятия.

Относительная устойчивость внешнего облика человека не означает, что на протяжении всей его жизнедеятельности ему будут присущи неизменные признаки внешности. На формирование внешнего облика могут повлиять различные факторы: закономерности развития и старения, наличие заболеваний, перенесение травм и повреждений, косметическая коррекция отдельных частей тела. Кроме этого, на внешность человека влияют и психические состояния личности, окружающая обстановка. Однако процесс идентификации человека по признакам его внешности — ограниченный и относительно недолгий процесс, в течение которого неизменность внешнего облика человека вполне реальна. Поскольку идентификация производится по совокупности выявленных сходств и различий, незначительные изменения во внешнем облике человека не будут иметь решающего значения.

Отражаемость (рефлекторность) [9, с. 6] внешнего облика человека — свойство, которое заключается в способности внешнего облика человека отображаться на различных носителях. Прежде всего это такая форма отражения, как запечатление мысленного образа в памяти воспринимающего лица. Кроме того, носители могут быть и материальные — портреты, фото- и видеоизображения, ориентировки, словесные портреты лиц, маски-слепки, скульптурные композиции. Все чаще средствами отображения являются устройства видеонаблюдения, что определяет дальнейшее исследование отображенных объектов. Как вполне справедливо отмечает А.М. Зинин, «система средств отображения внешнего облика человека на различных носителях информации наиболее активно пре-

терпевает изменения с учетом современных технологий. На экспертизу обычно поступают изображения, полученные с помощью аппаратуры для видеонаблюдения. Работа с кадрами видеозаписей как носителями портретной информации отличается своей спецификой: лица фиксируются под определенным ракурсом, могут быть также фрагментарные изображения лиц. В качестве средств фиксации используются фотокамеры, сопряженные со средствами мобильной связи. В связи с этим необходимо обратить внимание на факторы, влияющие на отображение внешнего облика человека с помощью таких средств» [10].

В этой связи представляется, что рассмотренный перечень свойств внешнего облика человека может быть дополнен еще одним — воспринимаемостью. Криминалистическое значение внешнего облика появляется лишь в том случае, когда он зрительно воспринимается другим человеком. Именно этот факт обусловливает дальнейшее отображение мысленного образа в памяти, закрепление в ней и, как следствие, идентификацию и диагностику. Воспринимаемость как свойство внешнего облика обозначает способность отдельных характеристик внешнего облика быть распознанными субъектом восприятия. К примеру, рисунок вен ладони человека не воспринимаем невооруженным глазом человека, а доступен для распознавания только соответствующим техническим устройством. Тот факт, что в настоящее время субъектом восприятия внешнего облика являются не органы чувств человека, а технические устройства (веб-камера, камера наружного наблюдения, видеорегистратор, сканер, тачскрин мобильного смартфона), стирает равенство между рефлекторностью и воспринимаемостью внешнего облика человека. Точность восприятия таких устройств выше, чем органа зрения человека, и позволяет воспринять не только видимые человеческому глазу признаки внешности, но и отдельные свойства слабовидимого характера. К последним можно отнести рисунок сетчатки глаза, а также рисунок вен на ладони. Аутентификация по данным признакам успешно применяется в биометрических технологиях, которые могут быть использованы и в процессе выявления и расследования преступлений.

Таким образом, представляется, что внешний облик человека — это сложная система элементов, в совокупности складывающихся во внешность человека — образ, который зрительно воспринимается другими людьми и техническими устройствами.

Традиционно во внешнем облике человека принято выделять две основные группы элементов:

1. *Общефизические признаки* (морфологические, анатомические, антропологические, статические). Это признаки, характеризующие внешность человека независимо от формы его жизнедеятельности: раса, национальность, телосложение, пол, возраст, строение отдельных частей тела и их выраженность. Особенностью общефизических признаков является их относительная устойчивость и неизменность на протяжении определенного жизненного периода и сохранение их после смерти (на период, предшествующий разложению мягких тканей). Иными словами, общефизические признаки внешнего образа присущи как живому человеку, так и трупу.

Представляется, что в систему анатомических признаков необходимо включить и биометрические признаки: геометрию рук, рисунок вен на ладонных поверхностях, пальцевую термограмму, геометрию лица и черепа и др. Так, Д.Ю. Писарев подчеркивает, что актуальными становятся вопросы биометрии в таких областях, как пограничный контроль, деятельность правоохранительных органов, транспортная безопасность, контроль доступа и перемещения в исправительных учреждениях, противодействие терроризму и экстремизму, защита информационных систем. Соответственно, и криминалистика начинает развиваться уже с учетом международных парадигм и в духе применения новейших технологий [11, с. 10]. К примеру, в последнее время широкое распространение получила система распознавания лиц в аэропортах и метрополитенах, основанная на сопоставлении биометрических параметров фотоизображения в паспорте и биометрических параметров лица человека, сканируемого специальным устройством. Существует более удобная система идентификационного токена, когда чип из паспорта представляется лишь единовременно, а лицо становится постоянным «паспортом человека», что существенно экономит время на организацию процедуры идентификации пассажира [12].

Важно, что биометрические характеристики общефизических признаков внешности человека могут быть использованы не только в идентификационных, но и в поисковых целях. Так, разработка Министерством внутренних дел РФ

Федеральной информационной системы биометрических учетов позволит выявлять разыскиваемых по лицу, радужной оболочке глаза и татуировкам, расположенным на открытых частях тела. Лидер по внедрению систем электронного распознавания лиц по биометрическим данным — Китайская Народная Республика, правоохранительные органы которой используют в практике не только более 600 млн камер наружного наблюдения, но и специальные персональные солнечные смарт-очки для сотрудников, которые позволяют распознать внешний облик человека на расстоянии до 5 м при условии восприятия не менее 70 % лица [13].

Российские правоохранительные органы также активно внедряют систему распознавания лиц в свою практику, однако эпидемиологическая ситуация, сложившаяся в связи с распространением новой коронавирусной инфекции COVID-19, вносит свои коррективы. Введение масочного режима сопряжено с сокрытием двух третей лица, что, безусловно, создает определенные сложности в работе системы, основанной не только на фиксировании рисунка радужной оболочки глаза, но и на фиксировании и сопоставлении черт лица. Кроме того, в российской действительности зачастую сокрытие большей части лица происходит не только по указанной выше причине, но и вследствие климатических условий (укутывание лиц шарфами и повязками), модных тенденций (ношение мужчинами щетин и бород, закрывающих всю нижнюю часть лица), а в некоторых регионах — особенностей религиозного характера (ношение женщинами костюмов, закрывающих лицо).

Еще одним существенным минусом, сказывающимся на криминалистической ценности исследования анатомических признаков, является их статичность, существенно упрощающая механизм фальсификации. Известны случаи сканирования и копирования фотоизображения, при котором сохраняется геометрия лица, для дальнейшей идентификации и неправомерного доступа к защищенной информации (информационным ресурсам), разработана техническая возможность выявления и изъятия отпечатка пальца, а также его моделирования [14].

Высокая степень информированности населения об идентификационной криминалистической значимости анатомических признаков приводит к разработке различных методов противодействия существующим технологиям. К примеру, каждый преступник осведомлен об индивидуальности и отображаемости отпечатков пальцев и предпринимает усилия, чтобы не оставить их, но лишь немногим известно о высокой криминалистической значимости отпечатков ушных раковин, в связи с чем усилия по их сокрытию предпринимаются редко.

В этой связи особое криминалистическое значение приобретает фиксация и исследование второй разновидности признаков внешнего облика человека.

2. *Функциональные (динамические) признаки* — это те элементы, которые становятся зрительно воспринимаемыми только лишь при определенных двигательных формах жизнедеятельности человека. К ним относятся походка, речь, жестикуляция, мимика, пантомимика, позы, привычки, манеры и др. По мнению некоторых авторов, возможности криминалистического исследования функциональных (динамических) признаков внешности человека в настоящее время используются не в полной мере, а ограничиваются в основном наблюдением или изучением статичных материально фиксированных отображений, таких как дорожка следов обуви, предметные следы-отображения профессиональных навыков при изготовлении тех или иных изделий, а также качественным описанием функциональных признаков без количественной их оценки [15, с. 35]. Безусловно, к числу причин сложившейся ситуации можно отнести сложности технического и методического характера. Однако, к примеру, разработки в области криминалистического исследования походки [16] и артикуляции человека [17] по материалам видеозаписи успешно используются в правоприменительной практике и позволяют намечать общие положительные тенденции в расширении возможностей криминалистического исследования функциональных признаков человека.

С учетом современных реалий представляется целесообразным дополнить систему динамических признаков внешнего облика человека еще одним элементом — поведением человека в цифровом пространстве (цифровым поведением).

Под поведением человека чаще всего подразумевается система внутренне взаимосвязанных действий, осуществляемых сложным объектом [18], внешняя и внутренняя активность человека во взаимоотношениях с окружающей средой. Цифровое поведение является разновидностью информационного поведения, под

которым предлагается понимать образ действий, совокупность усилий, предпринимаемых человеком для получения (усвоения) и использования (создания) нового знания, его передачи и распространения в обществе [19]. Особенностью цифрового поведения выступает использование устройств компьютерной техники и цифровых гаджетов как необходимого посредника в процессе передачи информации.

Человек, осуществляя активные действия по поиску, восприятию, анализу и исследованию информации, реализует совокупность поведенческих актов, являющихся внешним выражением мыслительной деятельности (паттернов поведения). При этом физически сложные разнообразные последовательные действия не производятся, а усилия по поиску, вводу или обработке цифровой информации концентрируются вокруг устройства. Однако при кажущемся однообразии осуществляемых действий цифровое поведение человека характеризуется совокупностью индивидуальных устойчивых признаков, способных отображаться в цифровых следах.

Представляется, что к числу наиболее криминалистически значимых элементов цифрового поведения можно отнести клавиатурный почерк, цифровой почерк и цифровую жестикуляцию.

Стилометрия (клавиатурный почерк) — это набор динамических характеристик при нажатии на клавиши клавиатуры компьютера, включающий в себя систему подсознательных автоматических действий, привычных пользователю. Наиболее важными из них являются динамика ввода (время между нажатием клавиш и временем их удержания), скорость набора (время, которое требуется пользователю для поиска нужного символа на клавиатуре), скорость ввода (результат деления количества символов на время печатания), интенсивность нажима (сила воздействия на клавишу клавиатуры), продолжительность и структура пауз и задержек, особенности реализации клавиш (использование клавиш для печатания определенных знаков — заглавных букв, кавычек, скобок и т.д.), частота ошибок при вводе.

Несмотря на относительную молодость данного способа, по оценкам исследователей, вероятность идентификации пользователя по клавиатурному почерку составляет 0,91 [20]. Исследование клавиатурного почерка имеет ряд преимуществ: невозможность передачи другому человеку (в отличие от секретного кода, шифра, ключа), отсутствие необходимости в применении сложной дорогостоящей аппаратуры, незаметность проверки для пользователя. Клавиатурный почерк предоставляет широкие возможности при диагностике цифрового автоподлога — ситуации, при которой недобросовестный пользователь инсценирует хищение личностной информации третьими лицами (например, лично осуществив списание со своего счета, утверждает, что стал жертвой мошенничества вследствие неправомерного доступа к банковскому счету).

Основной принцип распознавания клавиатурного почерка сводится к тому, что пользователю предлагается набрать контрольную фразу (текст), исследуемую с помощью различных методов, в основе которых лежит определение времени между событиями клавиатуры (т.е. нажатием кнопки и ее отпусканием). Идентификация пользователя строится на анализе длительности интервалов, соответствующих каждой комбинации клавиш [21, с. 179].

В настоящее время распознавание компьютерного почерка осуществляется в основном в целях аутентификации пользователя в рамках обеспечения информационной безопасности хранимых данных. Однако за рубежом метод распознавания компьютерного почерка активно используется в выявлении и расследовании преступлений. Так, в 2018 г. программа записи особенностей биометрии поведения при входе в учетную запись Королевского Банка Шотландии зарегистрировала необычную активность учетной записи одного состоятельного клиента. После аутентификации посетитель использовал колесо прокрутки мыши — то, чего клиент никогда раньше не делал. Затем пользователь ввел цифры с верхней части клавиатуры, а не с боковой, с которой обычно вводил клиент. Доступ к денежным средствам в аккаунте клиента был заблокирован. Впоследствии было установлено, что учетная запись была взломана. Распознавание компьютерного почерка позволило пресечь хищение семизначной суммы со счета клиента [22]. Российские банки также успешно внедряют в систему информационной безопасности технологии фиксации биометрии поведения, однако в настоящее время наибольшее распространение получила активная (статическая) биометрия: более 50 банков и финансовых организаций используют созданную ПАО «Ростелеком» при поддержке Банка России и Министерства цифрового развития Единую биометрическую систему («Ключ Ростелеком»).

Представляется, что научные разработки в области распознавания клавиатурного почерка могут и должны быть успешно использованы в сфере выявления, расследования и раскрытия преступлений против собственности и компьютерной информации.

Клавиатурный почерк — наиболее значимая разновидность *цифрового почерка*, в который, помимо закономерностей использования клавиш компьютерной клавиатуры, входят еще такие характеристики, как закономерности движения компьютерной мышью (особенности использования клавиш и колесика, их сочетание, амплитуда и радиус движения компьютерной мыши), навигационные привычки, а также особенности использования тачскрина смартфона (скорость, стиль взаимодействия и давления и т.д.).

Жестикуляция, мимика, движение губ. В отличие от традиционных одноименных динамических признаков внешнего облика жесты, мимика и движение губ как часть цифрового поведения человека фиксируются с помощью веб-камер или камер наружного наблюдения и представляют собой сформированные привычные движения при манипуляциях с компьютерной техникой и цифровыми устройствами. Так, форма движения губ при произнесении кодового слова, цифрового пароля с учетом структуры и мимики обладает индивидуальностью и выражается в особенностях видимой артикуляции, при этом внимание обращается не на смысловое содержание слова, пароля и его соответствие заданному, а именно на внешнее выражение речевой активности.

Жестикуляция как элемент цифрового поведения человека выражается в движениях рук при манипуляциях с цифровым устройством мобильного характера (чаще всего — смартфоном). Имеет значение угол, под которым удерживается смартфон, значение пальцев, которые использует подозреваемый для управления приложениями в гаджете, жесты и движения по управлению телефоном, а также паузы между ними.

Все упомянутые элементы цифрового поведения человека фиксируются и распознаются с помощью биометрического метода и получили название «биометрия поведения» (поведенческая биометрия[1], пассивная биометрия, тихая биометрия) [23]. Как и при традиционном методе криминалистической идентификации, в основе биометрии поведения лежит сравнение выявленной совокупности индивидуальных устойчивых признаков, характеризующих поведение лица (их подсчет, измерение и статистический анализ), с контрольными образцами, которые, как правило, хранятся в информационной базе данных. Применение математических и статистических методов при этом осуществляется специалистом посредством использования электронно-вычислительной техники.

К плюсам поведенческой биометрии можно отнести ее скрытый характер: испытуемый может не подозревать, что осуществляется фиксация его поведенческих характеристик, поскольку ему не объявляют о необходимости предъявить какие-либо факты либо осуществить какие-либо действия — он ведет себя естественно. Скрытый характер удобен при создании базы данных: не нужно осуществлять какие-либо технически сложные действия, привлекать большое количество специалистов.

Естественность поведения испытуемого — обстоятельство, которое обусловливает невозможность фальсификации поведенческих характеристик. Если отпечатки пальцев, форму лица и иных частей тела можно искусственно сконструировать, используя машинные методы, то поведение человека скопировать и воссоздать невозможно, поскольку оно комплексно, динамично и индивидуально.

Метод поведенческой биометрии научно должен основываться на ГОСТах, регламентирующих испытания биометрических технологий: ГОСТ Р ИСО/МЭК 19795-1-2007 «Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 1. Принципы и структура» (утвержден приказом Федерального агентства по техническому регулированию и метрологии от 25 декабря 2008 г. № 403-ст) и ГОСТ Р ИСО/МЭК 19795-2-2008 «Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 2. Методы проведения технологического и сценарного испытаний» (утвержден приказом Федерального агентства по техническому регулированию и метрологии от 18 декабря 2008 г. № 448-ст).

Использование поведенческой биометрии в практике правоохранительных органов не ограничивается исследованием только цифрового

[1] Behavioural biometrics: Online identification is getting more and more intrusive // The Economist. 2019. URL: https://www.economist.com/science-and-technology/2019/05/23/online-identification-is-getting-more-and-more-intrusive.

поведения, а включает в себя изучение и иных характеристик [24]. Так, в настоящее время к широкому внедрению готовятся биометрические исследования подписи, рукописного почерка, походки и голоса человека [25]. Использование метода поведенческой биометрии позволит не только решить идентификационные задачи и достичь поисковых целей, но и выполнить некоторые диагностические задачи — получить информацию о состоянии лица, его положении, возрасте, поле и других характеристиках.

Отсутствие научно обоснованной и практически апробированной методики исследования цифрового поведения не позволяет осуществлять назначение и производство соответствующих судебных экспертиз и исключает доказательственное значение полученной информации. Однако комплексный анализ выявленных характеристик даст возможность получить криминалистически значимую информацию, которую можно использовать в поисковых, познавательных, организационных и тактических целях.

Таким образом, криминалистическая габитоскопия представляет собой научно-методологический базис исследования цифрового образа и цифрового поведения человека в процессе выявления, расследования и раскрытия преступлений, систематизирует новейшие практические разработки и создает необходимые научные предпосылки для дальнейших исследований в обозначенной области. Расширение структуры и содержания криминалистической габитоскопии путем включения в перечень признаков внешнего облика закономерностей цифрового образа и поведения человека позволит не только сформировать научно-методологический базис применения новых методов исследования, но и обеспечить целостность криминалистической науки, предотвращая ее деление на электронную криминалистику, медицинскую криминалистику, экономическую криминалистику и т.п., что представляется не вполне целесообразным с учетом единства предмета и объекта криминалистики.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Егерева О.А. Некоторые вопросы расследования киберпреступлений / О.А. Егерева, В.В. Коломинов, М.С. Сизова // Сибирские уголовно-процессуальные и криминалистические чтения. — 2018. — № 4 (22). — С. 24–32.

2. Протасевич А.А. Особенности осмотра места происшествия по делам о киберпреступлениях / А.А. Протасевич, Л.П. Зверянская // Известия Иркутской государственной экономической академии (Байкальский государственный университет экономики и права). — 2013. — № 2. — URL: http://brj-bguep.ru/reader/article.aspx?id=17278.

3. Особенности расследования отдельных категорий уголовных дел и уголовных дел в отношении отдельных категорий лиц / под ред. И.Г. Смирновой. — Москва : Юрлитинформ, 2016. — 336 с.

4. Россинская Е.Р. Теория информационно-компьютерного обеспечения криминалистической деятельности: концепция, система, основные закономерности / Е.Р. Россинская // Вестник Восточно-Сибирского института МВД России. — 2019. — № 2 (89). — С. 193–202.

5. Степаненко Д.А. Цифровые технологии в криминалистическом обеспечении процесса доказывания / Д.А. Степаненко, А.А. Рудых // Криминалистика: теория и практика : материалы 7-й Междунар. науч.-практ. конф. — Краснодар, 2019. — С. 317–322.

6. Степаненко Д.А. Цифровая реальность и криминалистика / Д.А. Степаненко, В.В. Коломинов // ГлаголЪ правосудия. — 2018. — № 3 (17). — С. 38–43.

7. Зинин А.М. Габитоскопия и портретная экспертиза : курс лекций / А.М. Зинин. — Москва : Щит-М, 2002. — 157 с.

8. Фойгель Е.И. Современное состояние криминалистической габитоскопии / Е.И. Фойгель // Пролог: журнал о праве. — 2016. — № 2 (10). — С. 24–28.

9. Снетков В.А. Габитоскопия : учебник / В.А. Снетков. — Волгоград, 1979. — 183 с.

10. Зинин А.М. Проблемные вопросы изучения габитоскопии, основ производства судебных портретных экспертиз, изготовления субъективных портретов / А.М. Зинин // Энциклопедия Судебной Экспертизы. — 2019. — № 4 (23). — URL: http://www.proexpertizu.ru/theory_and_practice/portret/846.

11. Писарев Д.Ю. Проблемы применения биометрических систем в расследовании преступлений : автореф. дис. … канд. юрид. наук : 12.00.09 / Д.Ю. Писарев. — Краснодар, 2012. — 20 с.

12. Zorkadis V. On biometrics-based authentication and identification from a privacy-protection perspective. Deriving privacy-enhancing requirements / V. Zorkadis, P. Donos // Information Management & Computer Security. — 2004. — Vol. 12, № 1. — P. 125–137.

13. Dudley L. China's Ubiquitous Facial Recognition Tech Sparks Privacy Backlash / L. Dudley // The Diplomat. — 2020. — URL: https://thediplomat.com/2020/03/chinas-ubiquitous-facial-recognition-tech-sparks-privacy-backlash.

14. A critical insight into the identity authentication systems on smartphones / T. Mehraj, M.A. Sheheryar, S.A. Lone, A.H. Mir // Indonesian Journal of Electrical Engineering and Computer Science. — 2019. — Vol. 13, № 3. — P. 982–989.

15. Воецкая И.Н. Динамические признаки человека при решении идентификационных и диагностических задач. Существующие наработки и перспективы применения / И.Н. Воецкая // Актуальные проблемы радио- и кинотехнологий : материалы 2-й Междунар. науч.-техн. конф. — Санкт-Петербург, 2018. — С. 33–39.

16. Булгаков В.Г. Особенности методики судебно-экспертного исследования динамических признаков походки человека / В.Г. Булгаков, Е.В. Булгакова // Судебная экспертиза. — 2013. — № 4 (36). — С. 23–31.

17. Булгаков В.Г. Основы криминалистического исследования динамических признаков человека / В.Г. Булгаков. — Москва : Юрлитинформ, 2009. — 176 с.

18. Новая философская энциклопедия. В 4 т. / под ред. В.С. Степин. — Москва : Мысль, 2000–2001.

19. Дрешер Ю.Н. Изучение информационных потребностей и информационного поведения специалистов в структуре деятельности по обеспечению комфортной информационной среды / Ю.Н. Дрешер, Т.А. Атланова // Научные и технические библиотеки. — 2005. — № 11. — URL: http://ellib.gpntb.ru/subscribe/index.php?journal=ntb&year=2005&num=11&art=.

20. Григорьев В.Р. Использование статических методов для биометрической идентификации пользователя / В.Р. Григорьев, А.П. Никитин // Вестник РГГУ. Сер.: Информатика. Защита информации. Математика. — 2012. — № 14. — С. 135–142.

21. Иванов Д.А. Противодействие анализу клавиатурного почерка / Д.А. Иванов, А.П. Никитин // Вестник РГГУ. Сер.: Документоведение и архивоведение. Информатика. Защита информации и информационная безопасность. — 2014. — № 11 (133). — С. 178–183.

22. Клименко А. Поведенческая биометрия: наиболее эффективные решения в мире и Украине / А. Клименко // PaySpaceMagazine. — 2019. — URL: https://psm7.com/security/povedencheskaya-biometriya.html.

23. Wang L. Behavioural biometrics for human identification: intelligent Application / L. Wang, X. Geng. — Hershey : Medical Information Science Reference, 2010. — 505 p.

24. Анисимов Р. Поведенческая биометрия заменит пароли? / Р. Анисимов, В. Мамаев // Системы безопасности. — 2018. — № 2. — URL: http://lib.secuteck.ru/articles2/sys_ogr_dost/povedencheskaya-biometriya-zamenit-paroli.

25. Скобелев В. МВД при помощи камер начнет искать преступников по татуировкам и походке / В. Скобелев // РБК. — 2020. — 24 февр. — URL: https://www.rbc.ru/technology_and_media/24/02/2020/5e4fb5af9a7947cfdfd5e1e.

REFERENCES

1. Egereva O.A., Kolominov V.V., Sizova M.S. Some Questions of the Technique of the Investigation of Cyber Crimes. *Sibirskie ugolovno-protsessual'nye i kriminalisticheskie chteniya = Siberian Criminal Procedure and Criminalistic Readings*, 2018, no. 4 (22), pp. 24–32. (In Russian).

2. Protasevich A.A., Zveryanskaya L.P. Peculiarities of Cybercrime Scene Investigation. *Izvestiya Irkutskoi gosudarstvennoi ekonomicheskoi akademii (Baikalskii gosudarstvennyi universitet ekonomiki i prava) = Izvestiya of Irkutsk State Economics Academy (Baikal State University of Economics and Law)*, 2013, no. 2. Available at: http://brj-bguep.ru/reader/article.aspx?id=17278. (In Russian).

3. Smirnova I.G. (ed.). *Osobennosti rassledovaniya otdel'nykh kategorii ugolovnykh del i ugolovnykh del v otnoshenii otdel'nykh kategorii lits* [Specific Characteristics of Investigating Special Categories of Criminal Cases and Criminal Cases against some Specific Categories of Persons]. Moscow, Yurlitinform Publ., 2016. 336 p.

4. Rossinskaya E.R. Theory of Information and Computer Support of Criminalistic Activity: Concept, System, Basic Patterns. *Vestnik Vostochno-Sibirskogo instituta MVD Rossii = Vestnik of the Eastern Siberia Institute of the Ministry of the Interior of the Russian Federation*, 2019, № 2 (89), pp. 193–202. (In Russian).

5. Stepanenko D.A., Rudykh A.A. Digital technologies in the criminalistic support of the process of proofing. *Kriminalistika: teoriya i praktika. Materialy 7-i Mezhdunarodnoi nauchno-prakticheskoi konferentsii* [Criminalistics: Theory and Practice. Materials of the 7th International Scientific and Practical Conference]. Krasnodar, 2019, pp. 317–322. (In Russian).

6. Stepanenko D.A., Kolominov V.V. Digital Reality and Criminalistics. *Glagol pravosudiya = The Verb of Justice*, 2018, no. 3 (17), pp. 38–43. (In Russian).

7. Zinin A.M. *Gabitoskopiya i portretnaya ekspertiza* [Habitoscopy and Portrait Expertise]. Moscow, Shchit-M Publ., 2002. 157 p.

8. Foygel E.I. The Current State of Criminalistic Habitoscopy. *Prolog: zhurnal o prave = Prologue: Law Journal*, 2016, no. 2 (10), pp. 24–28. (In Russian).

9. Snetkov V.A. *Gabitoskopiya* [Habitoscopy]. Volgograd, 1979. 183 p.

10. Zinin A.M. Problem Issues of Studying Habitoscopy, Basis of Conducting Forensic Portrait Examination, Manufacture of Subjective Portraits. *Entsiklopediya Sudebnoi Ekspertizy = Encyclopedia of Forensic Sciences*, 2019, no. 4 (23). Available at: http://www.proexpertizu.ru/theory_and_practice/portret/846. (In Russian).

11. Pisarev D.Yu. *Problemy primeneniya biometricheskikh sistem v rassledovanii prestuplenii. Avtoref. Kand. Diss.* [The problems of using biometric systems in crime investigation. Cand. Diss. Thesis]. Krasnodar, 2012. 20 p.

12. Zorkadis V., Donos P. On biometrics-based authentication and identification from a privacy-protection perspective. Deriving privacy-enhancing requirements. *Information Management & Computer Security*, 2004, vol. 12, no. 1, pp. 125–137.

13. Dudley L. China's Ubiquitous Facial Recognition Tech Sparks Privacy Backlash. *The Diplomat*, 2020. Available at: https://thediplomat.com/2020/03/chinas-ubiquitous-facial-recognition-tech-sparks-privacy-backlash.

14. Mehraj T., Sheheryar M.A., Lone S.A., Mir A.H. A critical insight into the identity authentication systems on smartphones. *Indonesian Journal of Electrical Engineering and Computer Science*, 2019, vol. 13, no. 3, pp. 982–989.

15. Voetskaya A.N. Human Dynamic Characteristics to Solve Criminalistics Issues of Identification and Diagnostic. Existing Achievements and Perspectives of Application. *Aktual'nye problemy radio- i kinotekhnologii. Materialy 2-i Mezhdunarodnoi nauchno-tekhnicheskoi konferentsii* [Topical Issues of Radio and Movie Technologies. Materials of 2nd International Scientific Conference]. Saint Petersburg, 2018, pp. 33–39. (In Russian).

16. Bulgakov V.G., Bulgakova E.V. Peculiarities of Technique of Forensic Expert Examination of Dynamic Signs of a Human Gait. *Sudebnaya ekspertiza = Forensic Examination*, 2013, no. 4 (36), pp. 23–31. (In Russian).

17. Bulgakov V.G. *Osnovy kriminalisticheskogo issledovaniya dinamicheskikh priznakov cheloveka* [Basics of the Criminalistic Study of Dynamic Attributes of a Person]. Moscow, Yurlitinform Publ., 2009. 176 p.

18. Stepin V.S. (ed.). *Novaya filosofskaya entsiklopediya* [The New Encyclopedia of Philosophy]. Moscow, Mysl Publ., 2000–2001.

19. Dresher Yu.N., Atlanova T.A. Study of information needs and informational behavior of specialists in the structure of activities to ensure a comfortable information environment. *Nauchnye i tekhnicheskie biblioteki = Scientific and technical libraries*, 2005, no. 11. Available at: http://ellib.gpntb.ru/subscribe/index.php?journal=ntb&year=2005&num=11&art=. (In Russian)

20. Grigorev V.R., Nikitin A.P. Use of stationary methods for biometric identification of the user. *Vestnik RGGU. Seriya: Informatika. Zashchita informatsii. Matematika = RSUH Bulletin. Computer Science. Data Protection. Mathematics*, 2012, no. 14, pp. 135–142. (In Russian).

21. Ivanov D.A., Nikitin A.P. Counteraction against keyboard handwriting analysis. *Vestnik RGGU. Seriya: Dokumentovedenie i arkhivovedenie. Informatika. Zashchita informatsii i informatsionnaya bezopasnost' = RSUH Bulletin. Document and Archive Studies. Informatics. Information Protection and Information Security,* 2014, no. 11 (113), pp. 178–183. (In Russian).

22. Klimenko A. Behavior biometry: most effective solutions in the world and in Ukraine. *PaySpaceMagazine*, 2019. Available at: https://psm7.com/security/povedencheskaya-biometriya.html. (In Russian).

23. Wang L., Geng X. *Behavioural biometrics for human identification: intelligent Application*. Hershey, Medical Information Science Reference, 2010. 505 p.

24. Anisimov R., Mamaev V. Behavior biometry will substitute passwords? *Sistemy bezopasnosti = Security and Safety*, 2018, no. 2. Available at: http://lib.secuteck.ru/articles2/sys_ogr_dost/povedencheskaya-biometriya-zamenit-paroli. (In Russian).

25. Skobelev V. The Ministry of the Interior will use cameras to search for criminals by their tattoos and gait. *RBK = RBC*, 2020, February 24. Available at: https://www.rbc.ru/technology_and_media/24/02/2020/5e4fb5af9a7947cfdfd5e1e3. (In Russian).

ИНФОРМАЦИЯ ОБ АВТОРАХ

Протасевич Александр Алексеевич — директор Института государства и права Байкальского государственного университета, доктор юридических наук, профессор, заслуженный юрист Российской Федерации, г. Иркутск, Российская Федерация; e-mail: kupic@isea.ru.

Фойгель Елена Игоревна — заместитель директора Института государства и права Байкальского государственного университета по учебной работе, кандидат юридических наук, доцент, г. Иркутск, Российская Федерация; e-mail: foiguelelena@gmail.com.

ДЛЯ ЦИТИРОВАНИЯ

Протасевич А.А. О возможностях криминалистической габитоскопии при реализации мер противодействия современной киберпреступности / А.А. Протасевич, Е.И. Фойгель. — DOI: 10.17150/2500-4255.2020.14(3).471-480 // Всероссийский криминологический журнал. — 2020. — Т. 14, № 3. — С. 471–480.

INFORMATION ABOUT THE AUTHORS

Protasyevich, Alexander A. — Director, Institute of State and Law, Baikal State University, Doctor of Law, Professor, Honorary Lawyer of the Russian Federation, Irkutsk, the Russian Federation; e-mail: kupic@isea.ru.

Foygel, Elena I. — Deputy Director for Academic Studies, Institute of State and Law, Baikal State University, Ph.D. in Law, Ass. Professor, Irkutsk, the Russian Federation; e-mail: foiguelelena@gmail.com.

FOR CITATION

Protasevich A.A., Foygel E.I. On the scope of criminalistic habitoscopy in the implementation of measures against modern cyber crime. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2020, vol. 14, no. 3, pp. 471–480. DOI: 10.17150/2500-4255.2020.14(3).471-480. (In Russian).